

JA998173

JCS94 U.S. PTO
09/459287
12/17/99

#4

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出願年月日
Date of Application:

1998年12月28日

出願番号
Application Number:

平成10年特許願第372355号

出願人
Applicant(s):

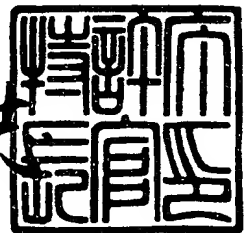
インターナショナル・ビジネス・マシーンズ・コーポレイシ
ョン

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 7月13日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



【書類名】 特許願

【整理番号】 JA998173

【提出日】 平成10年12月28日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 H04N 7/18

【発明の名称】 デジタルデータ認証システム

【請求項の数】 9

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 上條 浩一

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 森本 典繁

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 小出 昭夫

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 大和事業所内

【氏名】 阪倉 徹

【特許出願人】

【識別番号】 390009531

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【氏名又は名称原語表記】 INTERNATIONAL BUSINESS MACHINES CORPORATION

N

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【復代理人】

【識別番号】 100059258

【弁理士】

【氏名又は名称】 杉村 暁秀

【復代理人】

【識別番号】 100072051

【弁理士】

【氏名又は名称】 杉村 興作

【復代理人】

【識別番号】 100098383

【弁理士】

【氏名又は名称】 杉村 純子

【手数料の表示】

【予納台帳番号】 015093

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9304391

【包括委任状番号】 9304392

特平 10-372355

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルデータ認証システム

【特許請求の範囲】

【請求項1】 入力装置から入力されたデジタルデータをメモリ装置へ書き込むとともに、書き込まれたメモリ装置内のデジタルデータを受信装置へ転送するシステムにおいて、

(1) 入力装置からメモリ装置へのデジタルデータの書き込みおよびメモリ装置から受信装置へのデジタルデータの転送をする際に、入力装置とメモリ装置との間およびメモリ装置と受信装置との間それぞれで機器の認証を行い、

(2) メモリ装置にデジタルデータを書き込む際、デジタルデータに一方方向ハッシュ関数による電子署名を施すとともに、メモリ装置からデジタルデータを読み出して転送する際、施した電子署名を解読して、デジタルデータが記録時から改変がないことを確認した後転送する、

ことを特徴とするデジタルデータ認証システム。

【請求項2】 前記入力装置からメモリ装置へ書き込むべきデジタルデータ、および、メモリ装置から受信装置へ転送すべきデジタルデータに、機器認証データを織り交ぜる請求項1記載のデジタルデータ認証システム。

【請求項3】 前記入力装置および受信装置との認証、および、前記メモリ装置内でのデジタルデータへの認証および施した認証の解読を、メモリ装置に内蔵したCPUにより行う請求項1または2記載のデジタルデータ認証システム。

【請求項4】 前記入力装置とメモリ装置との間、および、メモリ装置と受信装置との間の認証が成功した場合のみ、前記入力装置からメモリ装置へのデジタルデータの書き込みおよび前記メモリ装置から受信装置へのデジタルデータの転送を行い、認証が成功しなかった場合は、通常のデジタルデータの書き込みおよび転送を行う請求項1～3のいずれか1項に記載のデジタルデータ認証システム。

【請求項5】 前記入力装置とメモリ装置との間では、両者の認証のために使用する特定の共通の暗号化関数Hdcと内部鍵Kdcを持ち、前記メモリ装置は、メモリ装置内の電子署名に使用するハッシュ関数Hcfと内部鍵Kcfを持ち、前記メモリ装置と入力装置との間では、両者の認証のために使用される特定の共

通の暗号化関数 $H_{p,c}$ とその鍵 $K_{p,c}$ を持つ請求項 1～4 のいずれか 1 項に記載のデジタルデータ認証システム。

【請求項 6】 前記関数 $H_{d,c}$ 、 $H_{c,f}$ 、 $H_{p,c}$ およびそれらの鍵 $K_{d,c}$ 、 $K_{c,f}$ 、 $K_{p,c}$ が、それぞれの装置の ROM に格納されている請求項 5 記載のデジタルデータ認証システム。

【請求項 7】 前記関数 $H_{p,c}$ が暗号化されて ROM に格納される請求項 6 記載のデジタルデータ認証システム。

【請求項 8】 前記入力装置からメモリ装置への認証を公開鍵方式を利用して行う請求項 1～7 のいずれか 1 項に記載のデジタルデータ記録システム。

【請求項 9】 前記メモリ装置がコンパクトフラッシュであり、前記ハッシュ関数によるデジタルデータの電子署名を、記録領域における各ページの ECC の計算の対象とならない冗長エリアに記憶する請求項 1～8 のいずれか 1 項に記載のデジタルデータ記録システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルカメラなどのデジタルデータ入力装置からデータの一時保管メモリを経由して転送されるデジタルデータの保全、つまり改ざんや改変防止のためのデジタルデータ記録システムに関するもので、特に、デジタルカメラによって撮影された損害保険の査定用デジタル写真や、建設現場における作業記録用のデジタル写真の改変防止をすることのできるシステムに関するものである。

【0002】

【従来の技術】

近年、デジタルカメラなど民生用デジタル機器の急速な普及により、多くの分野でデジタルデータの利用が進んでいる。しかし、デジタルデータは、痕跡を残さずにコンテンツを改変される危険性があるので、証拠として使うにはリスクを伴う。データの受け取り手が、データを信用するためには、データが取得されてから改変が無いことを保証する手段が必要となる。

【0003】

デジタル・データの改ざんや改変を防ぐ方法としては、MAC (Message Authentication Coding) など一方向ハッシュ関数によって作成した電子署名をデータに添付して転送する方法がある。デジタル画像の場合は、この電子署名を画像無いに電子透かしを使用して埋込画像との一体性をさらに高めることもできる（例えば、特開平 10-164549 号公報）。

【0004】

【発明が解決しようとする課題】

しかし、この技術が最も必要とされるデジタル写真への適用を考慮した場合、電子署名を施すのはカメラの中になる。その場合、カメラ側にかかる計算負荷が大きい上に、カメラ内に保管される暗号鍵は固定となるので、より信頼性の高いシステムが望まれる。つまり、現在の機器のハード的な制約の範囲内で実現可能で、かつ、必要十分なデータの保全性を確保できる方法が必要となっていた。

【0005】

本発明の目的は上述した課題を解消して、データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができるデジタルデータ認証システムを提供しようとするものである。

【0006】

【課題を解決するための手段】

本発明は、入力装置から入力されたデジタルデータをメモリ装置へ書き込むとともに、書き込まれたメモリ装置内のデジタルデータを受信装置へ転送するシステムが対象となる。このシステムにおいて、まず、入力装置からメモリ装置へのデジタルデータの書き込みおよびメモリ装置から受信装置へのデジタルデータの転送をする際に、入力装置とメモリ装置との間およびメモリ装置と受信装置との間それぞれで機器の認証を行う。同時に、メモリ装置にデジタルデータを書き込む際、デジタルデータに一方向ハッシュ関数による電子署名を施すとともに、メモリ装置からデジタルデータを読み出して転送する際、施した電子署名を解読して、デジタルデータが記録時から改変がないことを確認した後転送する。

【0007】

本発明では、まず、デジタルデータの入力装置からメモリ装置へのデータの書

き込み、および、メモリ装置から受信装置へのデータの転送をする際に、それぞれの機器の認証を行うことで、デジタルデータの入力装置からメモリ装置を介して受信装置へのデータ転送経路を限定することができる。また、メモリ装置にデータを記録する際、好ましくは内蔵のCPUによりデータを一方向ハッシュ関数により電子署名を施すことで、メモリ装置への直接アクセスによるデータの改変を防止することができる。これにより、データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができる。

【0008】

【発明の実施の形態】

図1は本発明のデジタルデータ認証システムの一例を説明するための図である。図1に示す例において、入力装置100はデジタルカメラ、メモリ装置200はコンパクトフラッシュ、受信装置300は画像データを管理するパーソナルコンピュータとした。メモリ装置200は着脱式に限定せず、カメラ内蔵のメモリでも同様である。なお、以下の説明において、「通常のデータ転送」というのは、認証を伴わない指定されていない装置との間でも正しく動作するデータ転送のことをいう。また、本発明に係る認証機能を持ったデジタルカメラをSDC (Secured Digital Camera) と、本発明に係る認証機能を持ったメモリ装置をSCF (Secured Compact Flash) と、本発明に係る認証機能を持ったパーソナルコンピュータをSPC (Secured Personal Computer) とする。さらに、DC、CF、PCは各々一般のデジタルカメラ、コンパクトフラッシュ、パーソナルコンピュータを示すものとする。

【0009】

まず、本発明のデジタルデータ認証システムを実行するにあたっての前提条件を説明する。始めに、特定された入力装置100、メモリ装置200および受信装置300の間では、特定の共通なコマンド (Request SeedコマンドとSend Seedコマンド) を定義する。一般の装置はこれらのコマンドに対し、エラーを返すかタイムアウトになる。Request Seedコマンドは、クライアントにシードを投げる事を要求するコマンドで、Send Seed コマンドは、クライアントにこれからシ

ードを投げる事を知らせるコマンドである。次に、特定された入力装置（SDC）100とメモリ装置（SCF）200の間では、特定の暗号化関数Hdcとその鍵Kdcを持っている。また、メモリ装置200はあるハッシュ関数Hcfと内部鍵Kcfを持っている。これらはそれぞれの装置のROMに格納されており、装置の外部に漏れる事はない。但し、この場合関数Hdc、Hcfは外部に漏れても機密性は保たれる。

【0010】

次に、特定されたメモリ装置（SCF）200と受信装置（SPC）300の間では、特定の共通の暗号化関数Hpcとその鍵Kpcを持っている。メモリ装置200においてKpcはNAND記録空間210に格納されているが、Kpcはある暗号化関数Exとその鍵Kxに因って暗号化されて格納されている。Hpc、Ex、Kxはそれぞれの装置のROMに格納されている。受信装置300でもKpcはある暗号化関数E2pcとその鍵パスワードに因って暗号化されている。パスワードはSCFの所有者のアクセスできないところに格納されているか、それ自体暗号化されている。その詳細は後述する。以下、図1を参照して各プロセスにおける各装置の機能を説明する。

【0011】

（1）デジタル画像のメモリ装置への記録について：

図1において、画像の取り込み部110で取得された画像は、画像処理部120を経由してメモリ装置200のNAND記録空間210に記録される。メモリ装置200は、入力装置100からのデータ書き込み要求がきた際、メモリ装置200の相互認証部231が内蔵のCPU220経由で入力装置100の相互認証部130に対して装置認証を行う。認証が成功した場合のみ画像処理部120からNAND記録空間210へのデータ記録が実行される。この認証は、セキュリティレベルを増すために、また、装置認証成功後に装置のすり替えができないように、データ転送の続く間も断続的に繰り返すよう構成することもできる。その内容については後述する。以下、実際の処理プロセスを説明する。

【0012】

（1. 1）SDCはCFに対してRequest Seedコマンドを投げ、ある乱数（=R

1) を要求する。この際、エラーが返ってくるか応答がない場合、SDCはCFがSCFでないと判断し、通常のデータ転送を行う。

(1. 2) SCFはR1をSDCに返す。シードを要求される前に通常のライトコマンドが来た場合、SCFはDCがSDCでないと判断し、通常のデータ転送を行う。

(1. 3) SDCはデータ転送を始める。CFは通常、1回のライトコマンドで1ページ(=512バイト)のデータ転送を最大256回繰り返す。

(1. 4) SDCは(1. 2)でR1がCFから返ってきた場合、R1を鍵Kdcを使って暗号化したR_Edを以下の式(1)で計算し、CFに返す。KdcはSDCとSCF間の秘密鍵である。

$$R_Ed = Hd_c(Kdc, R1) \quad \dots (1)$$

(1. 5) SCFは自分の持っているHdcとKdc、DCに送ったR1を使って上記式(1)の計算を行い、R_EdがDCから来たものと一致するかどうか確認する。R_Edが一致しなかった場合、DCはSDCでないと判断し、そのページも含め、今回のライトコマンドに対するデータ転送は、通常のデータ転送を行う。

【0013】

(2) メモリ装置内のデータ保護について：

上記(1. 5)でR_Edが一致した場合、SCFは更に、その次の認証が行われるまでの間に受け取りページに対して記録する画像に、CPUで生成した認証マーク(フラグ)を付加して電子署名を行い、NAND記録空間210に記録する。認証がない場合には認証マークを付加せずに記録する。CFは1ページにつき16バイトのECCの計算の対象とならない冗長エリアを有し、その内4バイトはリザーブドエリアのため、そのエリアに上記フラグを書くことができる。コンパクトフラッシュの詳細な構成については後述する。認証マークは送られてくるデータのハッシュを取ることで求めるが、データの全てに対してハッシュをとるとコストがかかる場合、ハッシュをかけるべきデータも暗号で決めれば良い。この際、データ全体でハッシュをとらない事によるセキュリティが心配されるが、通常、DCからのデータはJPEGで圧縮されており、部分(例えば1バイ

ト) 単位のスワップではデータ自体を改変するのは非常に困難なため、セキュリティは十分保たれると考えられる。ここで、ハッシュの計算には、SCFのROMに内蔵された各SCFにユニークな鍵であるKcfを使う。Kcfさえ秘密であれば、ハッシュ関数Hcf自体は秘密である必要はない。

【0014】

メモリ装置200は、データを受信装置300に転送する際に、内蔵のCPUによりデータの認証アルゴリズムHcfと非公開鍵Kcfを利用して画像に付された電子署名を解読し、画像が記録時から改変のないことを確認した後、後述するSCFとPC間の認証に対し、正しい答えを返す。改変が検出された場合、SCFとPC間の認証に対しエラーを返す。

【0015】

(3) メモリ装置から受信装置へのデータ転送について：

メモリ装置200のNAND記録空間210に記録されているデータは、受信装置300の記録空間310に転送される。この際、メモリ装置200の相互認証部232と受信装置300の相互認証部320との間で機器の認証が行われ、認証が成功した場合のみ、NAND記録空間210から記録空間310へのデータ転送が実行される。受信装置300は、メモリ装置200からデータを読み出す際に、メモリ装置200の相互認証部232に対して両方で共通の暗号化関数Hp cと受信装置300が指定する非公開の鍵Kp cをもとに認証を行い、正規の受信装置300であることを確認する。また、上述したように、メモリ装置200は、データを受信装置300に転送する際に、内蔵のCPUによりデータの認証アルゴリズムHcfと非公開の秘密鍵Kcfで画像が記録時からの改変のないことを確認した後、確認済みであることを示すデータを受信装置300へ伝達する。メモリ装置200の認証とメモリ装置200から伝達される「改変なし確認」の情報を拠り所に当該データが所定の入力装置100から限定された経路を通過してきたデータであることを確認することができる。以下、具体的なプロセスを示す。

【0016】

(3. 1) SPCはCFに対してSend Seed コマンドを投げ、ある乱数 (= R 2

) を投げる事を知らせる。

(3. 2) SPCはR2をCFに返す。

(3. 3) SPCはデータを読み始めるが、CFは通常1回のリードコマンドで1ページ(=512バイト)のデータ転送を最大256回繰り返す。

(3. 4) SCFは先ず、PCが読もうとしているデータにフラグが正しくついているかをHcfとKcfを使い確かめる。正しくない場合は、データは指定されずと判断して、今回のリードコマンドに対する認証に対してはエラーを返す。

(3. 5) SCFは、フラグが正しい場合、送られてきたR2に対し、以下の式(2)の計算を行い、R_EpをPCに返す。KpcはSCFとSPCとの間の秘密鍵である。

$$R_Ep = H_{pc}(K_{pc}, R2) \quad \dots (2)$$

(3. 6) SPCは自分の持っているHpcとKpc、CFに送ったR2を使って上記(2)式の計算を行い、計算したR_EpがSCFから来たものと一致するかどうか確認する。もし、一致しなかった場合、CFもしくはリードしようとしているデータは指定したものでないと判断する。

(3. 7) SPCは、R_Epの計算結果がCFから来たものと一致した場合、対象のリードデータに対して、全てリードし終わるまでリードコマンドを送る毎に最低1回はシードを送り認証をし、全てのページに対して認証が正しく行われた場合のみそのデータはSDCから改ざん無しでSCF経由で来たものと判断する。この一連の動作により、SPCは、受け取ったデータの入力元と改ざんの有無を確認する事が出来る。図2に上述したSDCからSCFを介してSPCへの認証およびデータの流れの概念を示す。

【0017】

次に、上述した本発明のデジタルデータ認証システムにおいて好適に使用できるコンパクトフラッシュの構造について説明する。コンパクトフラッシュは、1994年サンディスクより発表された小型不揮発性メモリで、PCMCIA-ATAコンパチブルで電氣的、メカ的にType IIのPCMCIAカードとして使用することが出来る。容量としては、4M、8M、16Mバイト等があり、デジタルカメラで撮られたJPEGイメージ(50kから100kバイト)の記憶な

ど幅広い用途がある。コンパクトフラッシュの大きな特徴は、小型で大容量でありながらCPUを内蔵している点にある。図3にコンパクトフラッシュの内部構造の一例を、図4に物理フォーマット仕様（8Mバイト）の一例を、図5にページモデルの一例を、それぞれ示す。本発明では、図5に示す冗長領域のReserved Area にフラグを書き込んでいる。

【0018】

以上で、本発明のデジタルデータ認証システムの主要な部分の説明が終了した。次に、その他の運用上の選択肢について、公開鍵による運用と認証セクターのマルチプレクスとPCにおけるKpcの暗号化の一例について説明する。まず、
(4) 公開鍵による運用について：

SDCとSCFの間の認証機構において、公開鍵方式を利用することにより、カメラの「なりすまし」による改ざん画像のSCFへの書き込みをより困難にすることができる。これは、カメラ側にチャレンジ用のデータを暗号化する秘密鍵、SCF側にカメラからの回答を認証するための公開鍵を持たせることで達成することができる。

【0019】

(5) 認証セクターのマルチプレクスについて：

装置の認証は、主体となる装置（SDCとSCFの場合はSCF、SCFとSPCの場合はSPC）が相手側の装置にチャレンジ用のデータを送り、所定の暗号化によって変換され、返送されてくるデータを手元の暗号によって確認することで完結する。装置の認証プロセスとその後のデータ転送が独立している場合には、認証の完了を見計らって別の入力装置につなぎかえることによって、装置の「なりすまし」ができる危険性がある。これを防ぐために、入力装置からは継続的に認証データを、転送データに織り交ぜて送るようにした。認証データを織り交ぜるルールは、チャレンジデータを暗号化したあとの回答（R__Ed、R__Ep）から生成するものとし、直接的な認証データの転送と、そのデータを転送するルールの双方で相手方の装置の認証を行う。

【0020】

(6) PCにおけるKpcの暗号化の一例について：

まず、本構成における限定条件は以下の通りである。

1. SDC、SCF内のROMの中身に対する攻撃に対しては、ROMのコードは外からは解析出来ず、ROMを分解しても中身の解析は出来ないtaper resistである。因って、この中に入っている鍵(Kdc、Kpc、Kcf、Kx)も攻撃することができない。

2. SPCにおけるアップロード用の暗号鍵KpcはSPCの管理者が管理していて、且つ、暗号化されているため、SCFの所有者には推測不可能である。万が一SCFの所有者がPCのアップロードプログラムを解読し、そのPC内のKpcを推測する可能性がある場合、以下の対策を講じることができる。

【0021】

(a) Kpcのインストール時

PCの管理者はKpcのインストール時に以下の式(3)によりKpcを暗号化したKpc'を計算し、PCに記憶する。

$$Kpc' = E2pc(\text{パスワード}, Kpc) \quad \dots (3)$$

ここで、E2pcはKpcを暗号化するための暗号化関数で、パスワードはPC管理者のみが知り得るパスワードである、また、パスワードを以下の式(4)によりハッシュしたパスワード'もPCに記憶する。この際、パスワード自体は記憶しない。

$$\text{パスワード}' = Hpsw(\text{パスワード}) \quad \dots (4)$$

ここで、Hpswは一方方向ハッシュ関数である。

【0022】

(b) SCFとSPCとの間の認証時

SPCの管理者はパスワードを入力する。SPCのアップロードプログラムは入力されたパスワードより(4)式を計算し、計算値が記憶されているパスワード'と一致した場合、以下の式(5)よりKpcを計算し、認証に使用する。

$$Kpc = D2pc(\text{パスワード}, Kpc') \quad \dots (5)$$

ここで、D2pcはE2pcに対する復号化関数で、任意の値x、yに対し、以下の式(6)が成立する。

$$x = D2pc(y, E2pc(y, x)) \quad \dots (6)$$

この方法により、悪意のある者がPCよりKpc'、パスワード'、E2pc、D2pc、Hpassを見つけ出す事に成功しても、そこからKpcを推測することは不可能である。

【0023】

上述した本発明の利点を以下にまとめる。

(1) SDCとSCFとの間、および、SCFとSPCとの間で、それぞれ機器の認証を行っているため、入力装置から受信装置までのデータ転送経路を限定することができる。

(2) SDCとSCFとの間、および、SCFとSPCとの間のデータ転送は、認証セクタをデータにマルチプレクスして、断続的に認証を行うことにより、装置の認証成功後に認証のない入力装置をすりかえることが防止できる。

(3) SCFのメモリ領域にデータを記録する際に、SCFのROM内の秘密の鍵を使ったハッシュ関数で署名を施すため、NAND記録空間210を分解し、改ざんしたデータに置き換えることを防止することができる。

(4) SDC、SPCとの認証鍵(Kdc、Kpc)は、ROM内の秘密鍵(Kx)により暗号化されているため、SCFのNAND記録空間210を分解しても盗み出すことはできない。

(5) 装置の認証が行われなかったり、失敗した場合でも、データは通常のCFと同様にNAND記録空間210に記録され、読み出されることができる。ただし、認証がつかない。

(6) 本発明のシステムは既存のハードウェアの内蔵プログラムの改造で実現可能なため、カメラメーカーへの負担も軽く、デファクト標準として市場に広まる事が期待できる。

【0024】

【発明の効果】

以上の説明から明らかなように、本発明によれば、安価で効果的にデジタルデータの入力装置と受信装置のデータの保全が保証でき、デジタル写真にも証拠能力をもたせることが可能となる。また、本技術の導入には、既存のハードウェアの内蔵プログラムの改造で実現可能なため、カメラメーカーの対応への負担も軽く

デファクト標準として市場に広まることが期待できる。また、転送データの安全性の観点からデジタル化を見合わせている企業などのデジタル化を促進することができる。

【図面の簡単な説明】

【図 1】 本発明のデジタルデータ認証システムの一例を説明するための図である。

【図 2】 本発明における認証およびデータの流れの概念を示す図である。

【図 3】 コンパクトフラッシュの内部構造の一例を示す図である。

【図 4】 コンパクトフラッシュの物理フォーマットの一例を示す図である。

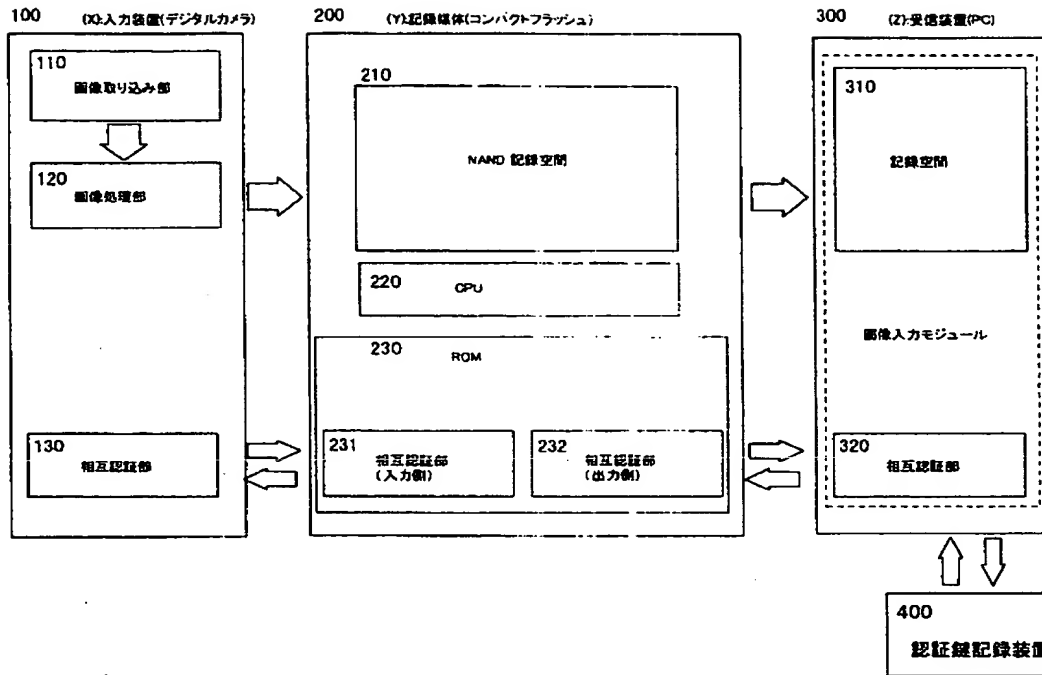
【図 5】 コンパクトフラッシュにおけるページモデルを示す図である。

【符号の説明】

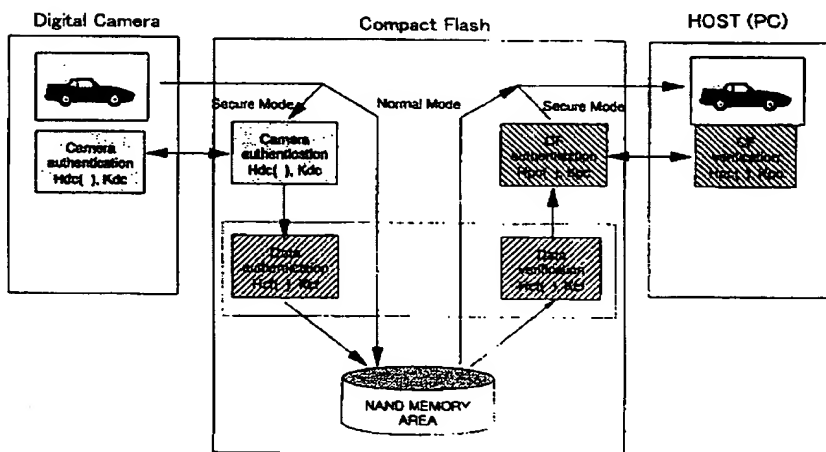
100 入力装置、110 画像取り込み部、120 画像処理部、130 相互認証部、200 メモリ装置、210 NAND記録空間、220 CPU、230 ROM、231、232 相互認証部、310 記録空間、320 相互記録部

【書類名】 図面

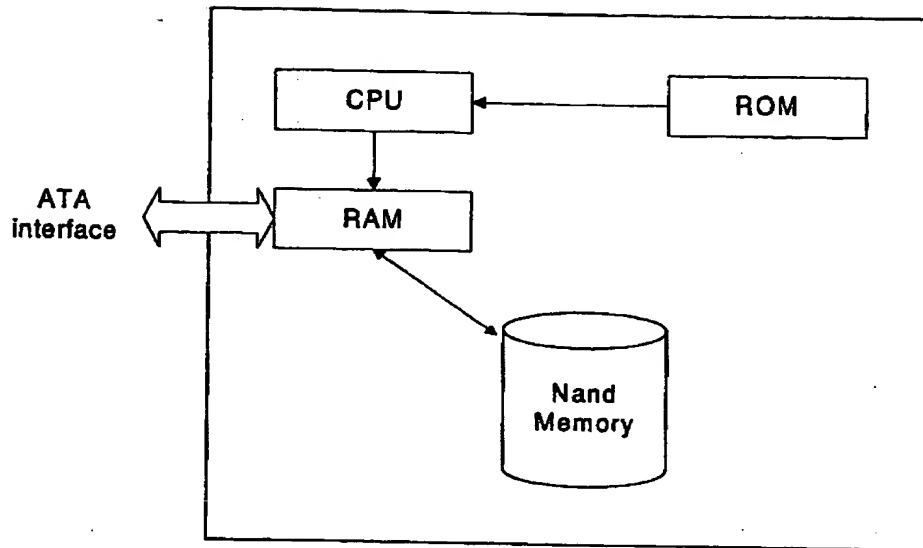
【図 1】



【図 2】



【図 3】



【図 4】

		0	511 512	527
Block 0	Page 0	データ領域 (512Byte)		冗長部 (16Byte)
	Page 1			
	:			
	Page 15			
Block 1	Page 0			
	Page 1			
	:			
	Page 15			
:	:			:
:	:			:
:	:			:
:	:			:
:	:			:
Block 999	Page 0			
	Page 1			
	:			
	Page 15			

【図 5】

◎データ領域 (512Byte)

Byte	全ページ
0 ～ 255	Data Area-1
256 ～ 511	Data Area-2

◎冗長領域 (16Byte)

Byte	全ページ
512	Reserved Area
513	
514	
515	
516	Data Status Area
517	Block Status Area
518	Block Address Area-1
519	
520	ECC Area-2
521	
522	
523	Block Address Area-2
524	
525	ECC Area-1
526	
527	

【書類名】 要約書

【要約】

【課題】 データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができるデジタルデータ認証システムを提供する。

【解決手段】 入力装置100からメモリ装置200へのデジタルデータの書き込みおよびメモリ装置200から受信装置300へのデジタルデータの転送をする際に、入力装置とメモリ装置との間およびメモリ装置と受信装置との間それぞれで機器の認証を行う。同時に、メモリ装置200にデジタルデータを書き込む際、デジタルデータに一方向ハッシュ関数による電子署名を施すとともに、メモリ装置200からデジタルデータを読み出して転送する際、施した電子署名を解読して、デジタルデータが記録時から改変がないことを確認した後転送する。これにより、データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができる。

【選択図】 図1

認定・付加情報

特許出願の番号	平成10年 特許願 第372355号
受付番号	59800854700
書類名	特許願
担当官	深沢 敏 2307
作成日	平成11年 2月22日

<認定情報・付加情報>

【特許出願人】

【識別番号】	390009531
【住所又は居所】	アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)
【氏名又は名称】	インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】	100086243
【住所又は居所】	神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	坂口 博

【代理人】

【識別番号】	100091568
【住所又は居所】	神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	市位 嘉宏

【代理人】

【識別番号】	100059258
【住所又は居所】	東京都千代田区霞が関3-2-4 霞山ビル7階
【氏名又は名称】	杉村 暁秀

【代理人】

【識別番号】	100072051
【住所又は居所】	東京都千代田区霞が関3-2-4 霞山ビル7階
【氏名又は名称】	杉村 興作

【代理人】

【識別番号】	100098383
【住所又は居所】	東京都千代田区霞が関3丁目2番4号 霞山ビルディング7階 杉村萬國特許事務所内

次頁有

認定・付加情報（続き）

【氏名又は名称】 杉村 純子

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 1990年10月24日

[変更理由] 新規登録

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレイション